UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,583	12/20/2001	Sven Anders Borje Svensson	4740-100	3277

24112 7590 03/29/2006

COATS & BENNETT, PLLC
P O BOX 5
RALEIGH, NC 27602

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/028,583	SVENSSON, SVEN ANDERS BORJE	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *35-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *35-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 35-60 have been considered.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/27/05 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 35-39,44, and 57-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant's admitted prior art (AAPA) in view of Howard, U.S. Patent Application Publication No. 2002/0118836.

As per claims 35,57,59, and 60, the applicant describes a method of authenticating a device with the following limitations which are met by AAPA and Howard:

a) receiving an authentication challenge from said first wireless network at said first device (AAPA: Specification, pages 1-2);

b) forwarding said authentication challenge from said first device to said second device (Howard: [0007]);

c) calculating an authentication response based on said authentication key at said second device (Howard: [0007]);

d) forwarding said authentication response from said second device to said first device (Howard: [0007]);

e) transmitting said authentication response from said first device to said first wireless network to authenticate said first device but not said second device to said first wireless network (AAPA: Specification, pages 1-2);

AAPA describes a method of authenticating a device in which a wireless network issues an authentication challenge to a first device. By providing an appropriate authentication response based on a calculation via an authentication key, the first device may be authenticated. AAPA, however, fails to disclose use of a second device to provide a calculation via an authentication key.

Howard discloses that a second device may provide calculations via an authentication key for a first device. More specifically, a first device may provide data to a second device. The second device is configured to encrypt/decrypt data as needed by the first device, and the second device maintains the cryptographic key internally [0007]. Furthermore, as taught by Howard, "by physically and operatively distributing the cryptographic processing/maintenance between the two devices, additional security is provided for protecting private data" [0007]. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Howard with those of AAPA because by doing so additional security is provided.

As per claims 36 and 58, the applicant describes the method of claims 35 and 57, which are met by AAPA in view of Howard, with the following limitation which is met by AAPA:

Wherein said first device is a computing device and said first wireless network is a WLAN (AAPA: Specification, pages 1-2).

As per claim 37, the applicant describes the method of claim 35, which is met by AAPA in view of Howard, with the following limitation which is met by Howard:

Wherein said second device is a cellular radiotelephone (Howard: [0034]).

As per claims 38 and 39, the applicant describes the method of claims 35 and 38, which are met by AAPA in view of Howard, with the following limitation which is met by Howard:

Wherein forwarding said authentication challenge and forwarding said authentication response occur across a communication interface connecting said first and second devices (Howard: [0035]).

As per claim 44, the applicant describes the method of claim 35, which is met by AAPA in view of Howard, with the following limitation which is met by AAPA:

Authenticating said first wireless device by said first wireless network based on said authentication response (AAPA: Specification, pages 1-2).

Claims 40 and 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Howard in further view of Proust (Proust, Albert. "O'Reilly Network – Personal Area Network: A Bluetooth Primer". Retrieved from www.oreillynet.com/pub/a/wireless/2000/11/03/bluetooth.html. 11/3/2000).

As per claims 40 and 42-43, the applicant describes the method of claim 38, which is met by AAPA in view of Howard, with the following limitation which is met by Proust:

Wherein said communication interface is a wireless communication interface (Proust: pages 1-3);

AAPA in view of Howard disclose all the limitations of claim 38. However, AAPA in view of Howard appear to be silent as to the communication interface being wireless. Proust discloses use of a wireless communication interface, which provides convenience as a physical, wired connection does not have to be made. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Proust with those of AAPA in view of Howard and use a wireless communication interface because doing so provides convenience as a physical, wired connection does not have to be made.

Claims 40 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Howard in further view of Saruta, U.S. Patent No. 4,959,874.

As per claims 40 and 41, the applicant describes the method of claim 38, which is met by AAPA in view of Howard, with the following limitation which is met by Saruta:

Wherein said communication interface is an optical interface (Saruta: Col 2, line 49 to Col 3, line 58);

AAPA in view of Howard disclose all the limitations of claim 38. However AAPA in view of Howard appear to be silent as to the communication interface being wireless. Saruta discloses use of a wireless communication interface, which provides convenience as a physical, wired connection does not have to be made. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Saruta with those of AAPA in view of Howard and use a wireless communication interface because doing so provides convenience as a physical, wired connection does not have to be made.

Claims 45-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Howard in further view of Menezes (Menezes, Alfred. Handbook of Applied Cryptography. Pages 31-32 and 403-405. CRC Press. 1997).

As per claim 45, the applicant describes the method of claim 44, which is met by AAPA in view of Howard, with the following limitation which is met by Menezes:

Wherein said authentication key comprises a shared key known to said first wireless network (Menezes: pages 31-32);

AAPA in view of Howard disclose all the limitations of claim 44. However, AAPA in view of Howard appear to be silent as to the type of encryption used in the system. Menezes discloses the well-known shared key encryption, which provides a number of advantages such as having a high rate of data

throughput and a strong cipher. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of AAPA in view of Howard and use shared key encryption in the system for at least the reasons that it affords a high rate of data throughput while providing strong protection of data.

As per claim 46, the applicant describes the method of claim 45, which is met by AAPA in view of Howard in further view of Menezes, with the following limitation which is met by AAPA:

a) using said authentication challenge and said shared key to compute an expected authentication response at said first network (AAPA: Specification, pages 1-2);

b) comparing said expected authentication response with the actual authentication response received from said first device (AAPA: Specification, pages 1-2).

As per claims 47-49, the applicant describes the method of claim 44, which is met by AAPA in view of Howard, with the following limitation which is met by Menezes:

Wherein said authentication key is a private key known only to the second wireless device, and wherein a public key corresponding to said private is known to the first wireless network (Menezes: pages 31-32; 403-405).

AAPA in view of Howard disclose all the limitations of claim 44. However, AAPA in view of Howard appear to be silent as to the type of encryption used in the system. Menezes discloses the well-known public key encryption, which provides a number of advantages such as allowing a private key/public key pair to remain unchanged for a considerable period of time and allowing the total number of keys in a network to be small. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of AAPA in view of Howard and use public key encryption in the system for at least these reasons.

Claims 50-51 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Howard in further view of Koster, U.S. Patent No. 6,259,914.

As per claims 50-51 and 56, the applicant describes the method of claim 35, which is met by AAPA in view of Howard, with the following limitation which is met by Koster:

a) forwarding said authentication response from said first wireless network to a second wireless network (Koster: Col 1, line 63 to Col 2, line 19);

b) authenticating said first device by said second wireless network based on said authentication response (Koster: Col 1, line 63 to Col 2, line 19);

AAPA in view of Howard disclose all the limitations of claim 35. However, AAPA in view of Howard fail to disclose use of a second wireless network in an authentication process. Koster discloses the idea that authentication information may be forwarded from a first wireless network to a second wireless network. A first device may be authenticated by the second wireless network. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Koster with those of AAPA in view of Howard because doing so makes the system more robust by allowing a device to function in a separate network from that which the authentication entity resides in.

Claims 52-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Howard in further view of Koster in further view of Menezes.

As per claims 52-53, the applicant describes the method of claim 51, which is met by AAPA in view of Howard in further view of Koster, with the following limitation which is met by Menezes:

Wherein said authentication key comprises a shared key known to said second wireless network (Menezes: pages 31-32);

AAPA in view of Howard in further view of Koster disclose all the limitations of claim 51. However, AAPA in view of Howard in further view of Koster appear to be silent as to the type of encryption used in the system. Menezes discloses the well-known shared key encryption, which provides a number of advantages such as having a high rate of data throughput and potential for a strong cipher. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine

the ideas of Menezes with those of AAPA in view of Howard in view of Koster and use shared key encryption in the system for at least the reasons that it affords a high rate of data throughput while providing strong protection of data.

As per claims 54-55, the applicant describes the method of claim 51, which is met by AAPA in view of Howard in further view of Koster, with the following limitation which is met by Menezes:

Wherein said authentication key is a private key known only to the second device, and wherein said private key has a corresponding public key that is known to the second wireless network (Menezes: pages 31-32, 403-405);

AAPA in view of Howard in further view of Koster disclose all the limitations of claim 51. However, AAPA in view of Howard in further view of Koster appear to be silent as to the type of encryption used in the system. Menezes discloses the well-known public key encryption, which provides a number of advantages such as allowing a private key/public key pair to remain unchanged for a considerable period of time and allowing the total number of keys in a network to be small. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of AAPA in view of Howard in view of Koster and use public key encryption in the system for at least these reasons.

Response to Arguments

Applicant's arguments, see Remarks filed 12/27/05, have been considered but are moot in view of the new ground(s) of rejection.

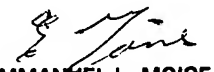
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS



EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER